**BRING YOUR OWN DEVICE (BYOD) POLICY**

| Last reviewed: | August 2025 |
|---|---|
| Next review due: | August 2026 |
| Reviewed by: | Director of Digital Strategy Head of IT (UK) |

## 1. Purpose and scope

### 1.1. Introduction

This policy is designed to support the responsible use of personal devices in school, enhancing and enriching the teaching and learning experience. It also outlines measures to protect students from harm, minimise risks to the school network, clarify user responsibilities, define acceptable and unacceptable use under the BYOD policy, and explain the possible consequences of not adhering to the rules

### 1.2. Scope

This policy applies to all students and staff who bring personal electronic devices onto d'Overbroeck's premises or connect them to the school's digital systems (on-site or remotely)

### 1.3. Definitions

**BYOD**: The use of personally owned devices (eg, laptops, tablets, mobile phones) for educational or work purposes.

**Device**: Any privately owned, internet-enabled electronic device.

**school Network:** d'Overbroeck's IT infrastructure, including wired and wireless networks, internet access, and internal systems.

**User**: is any individual granted authorisation to use BYOD. Users may include students, staff, volunteers, visitors, contractors, or individuals employed by the school directly or indirectly.

## 2. Acceptable devices

Permitted devices include:

- Smartphones

- Tablets

- Laptops

- E-readers (for academic use only)

- Smartwatches (in limited, non-disruptive use)

Devices must:

- be in full working order;

- be capable of supporting secure connections and updates;

- not be jailbroken or rooted (to avoid security risks).

**3. Permissions and usage rules**

3.1. **Students — Permitted use**

Students may:

- use devices during lessons only with the teacher's explicit permission;

- access digital learning resources, emails, research tools, and d'Overbroeck's platforms;

- use devices during break or lunch in designated areas, for appropriate activities only;

- use headphones when required for learning, if authorised by a teacher.

3.2. **Students — Prohibited use**

Students must NOT:

- access or attempt to bypass d'Overbroeck's filters or use unauthorised VPNs;

- use mobile data or personal hotspots while on school premises;

- use devices for gaming, social media, or messaging during lessons unless directed by a teacher;

- use devices in toilets, changing rooms, or other private areas;

- photograph, record, or film other students or staff without clear and explicit consent;

- share or upload school-related images, videos or content to public platforms without consent. Even if such permission is obtained images must under no circumstances be used to ridicule, harass, bully or abuse another person in any way.

- violate copyright law;

- access protected areas of computers at the school or anywhere else, ie, hack.

- allow others to use their device, or access another person's device or account.

3.3. **Staff — Permitted use**

Staff may:

- use personal devices for work-related tasks, communication, lesson delivery and planning;

- access d'Overbroeck's systems securely, including email and academic platforms;

- use approved apps and platforms in line with safeguarding and data protection requirements.

3.4. **Staff — Prohibited use**

Staff must NOT:

- store or access confidential or safeguarding data without encryption or proper authorisation;

- use personal messaging services (eg, WhatsApp, Instagram DMs) to communicate with students;

- allow students to access or use their personal devices;

- share or store school-related data on non-secure cloud platforms (eg, personal Dropbox, Google Drive).

4. **Network and internet use**

- All personal devices **must connect only** to d'Overbroeck's secured, filtered Wi-Fi network.

- Use of the network implies acceptance of this policy and the school's Acceptable Use Policy (AUP).

- Devices must not be used to:
  - disrupt or damage the network;
  - introduce unauthorised software, malware, or viruses;
  - access or share extremist, violent, illegal, or age-inappropriate material (as defined under the **Prevent Duty** and school safeguarding procedures).

5. **Security, data protection and privacy**

- Devices must be secured with a strong passcode, biometric lock or PIN.

- Staff and students **must not store** personal data, student records, or safeguarding information on personal devices unless authorised and encrypted.

- d'Overbroeck's may remotely restrict or monitor access to its systems from any device.

- The school may inspect or request access to personal devices in the event of:
  - a safeguarding concern;
  - suspected policy breach;
  - cyberbullying or misuse.

Such actions will be conducted with due respect to individual privacy and in accordance with the **UK GDPR** and the **Data Protection Act 2018**.

6. **Safeguarding, online safety, and Prevent**

- Personal devices must not be used to bully, harass or insult any other person inside or outside the school. Cyberbullying will bring severe penalties in accordance with our Behaviour policy and Anti-bullying policy.

- All users must report concerns about inappropriate content, cyberbullying, grooming, or radicalisation to the **Designated Safeguarding Lead (DSL)** immediately.

- Use of personal devices must never compromise student wellbeing, school security, or compliance with the **Prevent Duty.**

7. **Device responsibility and support**

- Students and staff are responsible for:
    - keeping devices secure, charged and in good condition;
    - ensuring regular updates and use of antivirus software;
    - protecting their data.

- d'Overbroeck's:
    - will offer **limited technical support** (eg, connecting to Wi-Fi, login issues);
    - will not be held liable for **loss, damage or theft** of personal devices on school premises.

Personal devices remain the responsibility of their owners at all times. The school cannot be held responsible for any theft, loss of, or damage to such devices whilst on school premises.

8. **Misuse and sanctions**

Breaches of this policy may result in:

- temporary or permanent withdrawal of BYOD privileges;
- confiscation of the device (returned only to a parent/guardian in the case of students);
- detention, suspension, or exclusion for serious or repeated breaches;
- referral to safeguarding authorities or police, where appropriate.

9. **Related policies and documents**

Available from the policies page of the school website:

- Anti-bullying policy
- Behaviour, rules, rewards and sanctions policy
- E-Safety Policy
- Safeguarding and promoting the welfare of children policy

Available to staff from the policies page of SharePoint:

- Acceptable use of IT policy for staff

*